I claim:

1. A method of tracking-back a malicious data packet in a connection-oriented communication network, comprising the steps of:

a) for a given time window (*Time Period*), computing a unique flow identifier (*FlowId*) for each packet of a given flow seen by a router interface (*Incoming Link*) at a network node;

b) inserting said *FlowId* into a data structure associated to said *Time Period* and said *Incoming Link,* available at said network node;

c) storing said data structure in a searchable repository; and

d) repeating steps a) to c) for a next *Time Period* and for each *Incoming link* at said network node.

2. The method of claim 1, further comprising:

e) determining the time of arrival *X* of said malicious packet at said network node and computing *FlowId* for said malicious packet; and

f) identifying said *Incoming Link* for said malicious packet by searching for the *FlowId* of said malicious packet in all data structures for said network node that cover the time of arrival *X*.

3. The method of claim 2, further comprising tracing-back hop by hop the source of said single packet from said router, by performing steps e) and f) for each network node along the path of said malicious packet.

4. The method of claim 1, wherein step a) is based on flow definition adopted for said network.

5. The method of claim 1, wherein step a) comprises applying a specified function to one or more header fields of each packet received in said flow.

6. The method of claim 1, wherein step a) comprises applying a specified function to one or more header fields of each packet received in said flow and an incoming interface identification parameter. .

7. The method of claim 1, wherein step a) comprises applying a specified function to one or more characteristics of each packet.

8. The method of claim 1, wherein step a) comprises applying a specified function to one or more characteristics of each packet received in said flow and an incoming interface identification parameter.

9. The method of claim 1, wherein said data structure is a hash table based on a Bloom filter.

10. The method of claim 1, wherein said searchable repository is maintained for each router interface at said network node.

11. The method of claim 10, wherein said searchable repository stores all said data structures for all router interfaces at said network node.

12. The method of claim 1, wherein said searchable database is a centralized searchable repository maintained for said network.

13. A method of tracking-back a malicious data packet in a connection-oriented communication network, comprising the steps of:

a) for a given time window (*Time Period*), computing a flow identifier (*FlowId*) for a flow seen by a router interface (*Incoming Link*) at a network node based on a flow characterization parameter obtained from a flow management system;

b) inserting said *FlowId* into a data structure, associated to said *Time Period* and said *Incoming Link,* available at said network node;

c) storing said data structure in a searchable repository; and

d) repeating steps a) to c) for a next *Time Period* and for each *Incoming link* at said network node.

14. A system for tracking-back a malicious data packet in a connection-oriented communication, comprising:

means for computing a unique flow identifier *FlowId* for each packet of a flow seen by a router interface (*Incoming Link*) at a network node over a given period of time (*Time Period*);

means for inserting said *FlowId* into a data structure associated to said *Time Period,* and said *Incoming Link* available for said network node;

a searchable repository for storing said data structure; and

a search engine for finding in said searchable repository the *Incoming Link* for said malicious packet based on a *FlowId* and a time of arrival *X* of said malicious packet.

15. The system of claim 14 further comprising a flow-based monitoring system for tracking back hop-by-hop the source of said malicious packet

16. The system of claim 14, wherein one said searchable repository is maintained for each interface at said network node.

17. The system of claim 14, wherein one said searchable repository is maintained for said network node.

18. The system of claim 14, wherein said searchable repository is a centralized database maintained for said network.

19. The system of claim 14, further comprising a flow based monitoring system for providing a flow characterization parameter to said means for calculating.

20. The system of claim 14 further comprising a flow management system for generating a flow characterization parameter.

21. The system of claim 20, wherein said means for computing is a *FlowId* calculator for computing said *FlowId* form one or more of packet header fields, packet characterization parameters and interface identification information.

22. The system of claim 20, wherein said means for computing is a *FlowId* calculator for computing said *FlowId* form packet header information.